

MESTRADO EM DIREITO E SEGURANÇA

MS 104/B – CIBERSEGURANÇA

FICHA DE UNIDADE CURRICULAR

1 – INFORMAÇÕES GERAIS

Coordenador: Prof. Doutor Jorge Bacelar Gouveia

Regente: Prof. Doutor Armando Marques Guedes (4h); Mestre Lino Santos (6h);

Mestre André Cabral Costa (4h)

Ano letivo: 2016/2017

Curso: 2.º Ciclo

Semestre: 2.º

ECTS: 5

Horas de contacto: 15

Contacto do docente: armandomarquesguedes@fd.unl.pt

Horário: 18:00-21:00

2 – OBJETIVOS

Esta unidade curricular pretende dotar os discentes do Mestrado em Direito e Segurança dos principais conceitos associados à cibersegurança, nos domínios da Sociologia e das Ciências jurídicas. Pretende igualmente dotar os discentes com o estado da arte das políticas públicas em matéria de cibersegurança no contexto Europeu e nacional e enquadrar a cibersegurança no conceito alargado de segurança nacional.

3 – PROGRAMA

1. Ciberespaço e ciber'espaços' (4h)

Génese, ontologia e teleologia. Espaço técnico, social e cultural. Geopolítica do ciberespaço.

2. Ciberconflitualidade e Cibersegurança (4h)

Hackers e outros fora-da-lei do mundo digital. Hacktivismo, Cibercrime organizado, Ciberterrorismo, Ciberespionagem e Ciberguerra. Enquadramento jurídico dos ciberataques.

3. Contra ciberconflitualidade e Políticas públicas de cibersegurança (3h)

Construção social da Cibersegurança. Domínios de actuação: Protecção simples, prossecução criminal, defesa do estado e diplomacia. Determinantes para uma Estratégia nacional de cibersegurança. A Estratégia portuguesa de Segurança do Ciberespaço.

4. Regulação do ciberespaço (3h)

Neutralidade da internet: oportunidades e limites. Vestfaliarização do ciberespaço. Sociedade vigilante. Convenção do cibercrime. Diretiva SRI e os seus desafios. O novo Regulamento Geral para a Protecção de Dados (RGPT-GDPR) recentemente aprovado pela a UE e os seus impactos previsíveis.

5. Cibersegurança empresarial (2h)

Sensibilização. Normas e boas práticas. Protecção de infraestruturas críticas. Resposta a incidentes

4 – BIBLIOGRAFIA

- Regulamento Geral de Protecção de Dados (2018), “2018 EU revision of data protection rules”, in

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

- Bacelar Gouveia, J. (2018), *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo*, Almedina.

- Clarke, R. A. & Knake, R. K. (2011). *Cyber war*. HarperCollins.

- Demchak, C. C. & Dombrowski, P. (2011). Rise of a cybered westphalian age. *Strategic Studies*, 5(1), 32-61.

- Denning, D. E. R. (1999). *Information warfare and security*. Reading MA: Addison-Wesley.
- Gozzi Jr, R. (1994). *The cyberspace metaphor*. Etc.: A Review of General Semantics, 51(2), 218.
- Klimburg, A. (2011). *Mobilising cyber power*. Survival, 53(1), 41-60.
- Libicki, M. C. (2012). *Cyberspace is not a warfighting domain*. ISJLP, 8, 321-336.
- Luijff, E., Besseling, K., & De Graaf, P. (2013). *Nineteen national cyber security strategies*. International journal of critical infrastructures, 9(1), 3-11.
- Marques Guedes, A. (2007). *Ligações Perigosas. Conectividade, Coordenação e Aprendizagem em Redes Terroristas*, Almedina, Coimbra [reviewed by Major-General J.M. Freire Nogueira, Segurança e Defesa 7].
- Marques Guedes, A. (2009). *As 'redes sociais' digitais, a participação 'política' e a segurança*, Pessoas e Territórios, 2: 44-45, Governo Civil de Lisboa
- Marques Guedes, A. (2010). *Geopolitica del Ciberspazio*, Quaderni Speciali di Limes. Rivista Italiana di Geopolitica: 187-199, Roma.
- Marques Guedes, A. (2010). *The new geopolitical coordinates of cyberspace*, Revista Militar, 2503/2504: 825-849, Lisboa.
- Marques Guedes, A. (2017). "Em rede. Os cabos de fibras ópticas submarinas e a centralidade portuguesa crescent num autêntico mar de conectividades", in *Revista de Marinha*, special no. 1000, pp. 20-27, Lisboa.
- Marques Guedes, A. (2018). Valor estratégico e económico dos cabos submarinos", in *Jornal da Economia do Mar*, 19, no. especial de aniversário, pp. 9-12.
- Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. PublicAffairs.
- Nye Jr, J. S. (2010). *Cyber power*. Technical report, Belfer Center for Science and International Affairs, Harvard Kennedy School.
- O'Connell, M. E. (2012). *Cyber security without cyber war*. Journal of Conflict and Security Law, 17(2), 187-209.
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press, USA.
- Santos, L. e Armando Marques Guedes (2016), "Breves Reflexões sobre o Poder e o Ciberespaço", com Lino Santos, *Revista de Direito e Segurança*, no. 6, pp. 189-210.

- Santos, L. (2012). Contributos para uma Melhor Governação da Cibersegurança em Portugal. In J. Bacelar Gouveia (ed.), *Estudos Avançados de Direito e Segurança* (Vol. II, pp. 217-205). Almedina.
- Schmitt, M. (1999). *Computer network attack and the use of force in international law: thoughts on a normative framework*. Columbia Journal of Transnational Law, 37, 887-937.
- Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
- Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. Penguin.
- Strate, L. (1999). *The varieties of cyberspace: Problems in definition and delimitation*. Western Journal of Communication, 63(3), 382-412.
- Subramnian, Samantha (2017). *Inside the Macedonian Fake-News Complex*. Wired, disponível em <https://www.wired.com/2017/02/veles-macedonia-fake-news/>
- Van De Velde, Jacqueline (2017). *The Law of Cyber Interference in Elections*. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828
- West-Brown, M. J. et al. (2003) *Handbook for Computer Security Teams (CSIRTs)*, CMU.

5 – AVALIAÇÃO

Exame final ou trabalho escrito.